National Cyber Security Centre
a part of GCHQ

MAIL CHECK
a part of the Secure Email Project

Mail Check: Helping councils to deal with spoof email

Case study: How UK councils are protecting their service users from spoof email

At a glance:

- Lowers the risk of council residents being targeted by cyber attack
- Raises trust in councils' communications, brand & reputation
- Increases the efficiency of council email campaigns and digital services
- Simplifies compliance with GDPR and other regulation
- ⅔ of councils now have a DMARC policy of quarantine/reject, so spoofed email sent from their domains is sent to spam (or rejected)

Local authorities are one of the trusted brands spoofed by cyber criminals. Mail Check makes it harder for attackers to spoof council emails by helping technical staff to set up and maintain good SPF, DKIM and DMARC configurations. As a result, councils across the UK are confident that legitimate sources of email are delivered to recipients' inboxes, whilst customers are more confident that they're dealing with local authorities, and not cyber criminals.

Council domains are high value targets

Attackers are known to be 'spoofing' trusted government email sending systems, including the local government sector. They can make their emails look like they're coming from you and your partner organisations. Successful email spoofing can harm your organisation through the loss of data, service provision and network availability. Your organisation, supply chain and communities can be put at risk in the event of a successful attack, through the spread of malware and data loss or theft.

Councils need to make it difficult for fake emails to be sent from all their domains. This is achieved through configuring effective anti-spoofing controls on all domains, including parked ones and where councils use cloud email such as Google G Suite and Microsoft Office 365.

Protecting you and your customers

Mail Check is a free tool from the National Cyber Security Centre, designed to help you make your email systems as secure as possible. With Mail Check, you can analyse the data from your email traffic to understand how emails are being sent and - crucially - identify if they're being abused. The results from this can then be used to tweak your email settings to achieve the security assurance you need.

Put simply, Mail Check makes it harder for attackers to spoof you by helping you to set up and maintain good Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting & Conformance (DMARC) configurations.

Here's how Mail Check is helping four local authorities to configure anti-spoofing controls on all their domains.

1. Gravesham Borough Council

Gravesham Borough Council has implemented a DMARC policy of **p=reject**, and therefore fake email is not delivered to recipients. Their IT team works in collaboration with all department heads and the Data Protection Officer to ensure that all sources of legitimate emails are added to their SPF record.

Their Assistant Director advises that they are consulted on all GDPR data protection information assessments (DPIA), so they get to see all sources of data, how it is being processed, and whether they need to add the IP addresses of mass mailing agents to their SPF record. It's a council-wide team effort, and not just an IT team one.

2. Chorley Council

Having implemented a DMARC policy of **p=quarantine**, Chorley are confident that spoof email is sent to spam folders, and legitimate email is being delivered to the intended recipients. This wisely provides the council time to monitor email traffic from their domains, and tweak the email settings accordingly.

In addition, managing their own DNS (and not relying on a third party helpdesk system) expedites their updates. Emma Marshall, ICT Service Lead at Chorley Council, says they view the project "as a business fix, not just an IT fix".

3. Merthyr Tydfil County Borough Council

Drawing upon resources from across the council and within the Welsh WARP (Warning, Advice and Reporting Point) helped Merthyr Tydfil County Borough Council quickly get ahead of the game and implement DMARC policy of **p=reject**. From the outset, they were clear that the key aim was to protect people from spoof emails.

4. Xentrall

Xentrall Shared Services is a public sector partnership wholly owned by **Stockton-on-Tees Borough Council**, **Darlington Borough Council** and **Tees Valley Combined Authority**, set up to deliver key back office transactional services. It supports 4,500 ICT users across 85 sites and together, they have implemented DMARC policies of **p=reject** on all the councils' domains.

"Gravesham council is continuing to move more and more towards digital working. Mail Check provides 'digital re-assurance', it means our customers are more confident that they're liaising with us, and not with cyber criminals."

Darren Everden
Assistant Director
Gravesham Borough Council

"We have increased confidence that legitimate sources of email, including mass email campaigns, are delivered to the recipients' inboxes, and not to their junk/spam folder."

Ryan James
Corporate Information Security Officer / ICT Team
Merthyr Tydfil County Borough Council

"We send out 530,000 emails a year and receive 1.4 million. We'd had some near misses in the past, with ransomware sent from external parties masquerading as senders from within our own organisation, which has caught some users off guard. Thanks to Mail Check, spam has decreased significantly, and we no longer receive any email from external malicious bodies purporting to come from us."

Chad Gray
Senior Technical Engineer
Chorley Council

"You need to know from where you send your email, for example you may use Office 365. Don't forget if you use services such as Mailchimp you will need to add these to your SPF record."

David Barr
ICT Solutions Architect
Xentrall Shared Services (Council owned)

From the outset, Xentrall Shared Services gained senior management sponsorship and worked with all departments and critically the ICT Information Security team.

Xentrall Shared Services read documentation from SOCITM (society for innovation, technology and modernisation) and the NCSC's online guidance. They used tools to help with correctly configuring the anti-spoofing controls, and they also worked with colleagues and reviewed data to ensure that all legitimate sources of email were added to their SPF records.

Find out more

If your organisation hasn't signed up to Mail Check yet, you can do so by visiting mailcheck.service.ncsc.gov.uk . You can also read the NCSC's guidance on email security and configuring anti-spoofing controls by visiting ncsc.gov.uk/collection/email-security-and-anti-spoofing .